universitätsverlag
ilmenau

Karla, Jürgen; Schmitt, Sebastian:

Begünstigt die Individualisierung der Mediennutzung im Web 2.0 den Datenmissbrauch? Eine Betrachtung der Risikopotenziale

URN: urn:nbn:de:gbv:ilm1-2009100077-p053-0

URL: http://nbn-resolving.de/urn:nbn:de:gbv:ilm1-2009100077-p053-0

Erschienen in:

Individualisierte Nutzung der Medien : Tagungsband Medienforum Ilmenau 2008 ; Technische Universität Ilmenau, 20. - 21. Juni 2008. - Ilmenau : Univ.-Verl. Ilmenau, 2009. - S. 53-74.

ISBN: 978-3-939473-55-8 [Druckausgabe]
URN: urn:nbn:de:gbv:ilm1-2009100077
URL: http://nbn-resolving.de/urn:nbn:de:gbv:ilm1-2009100077

Jürgen Karla & Sebastian Schmitt

Begünstigt die Individualisierung der Mediennutzung im Web 2.0 den Datenmissbrauch?

Eine Betrachtung der Risikopotenziale

1. Einleitung

Web 2.0-Publikumsdienste und Social Software tragen derzeit zu einem erheblichen Wandel des Verhaltens der Nutzer im Internet bei (Alby 2007: 16). Die Geschwindigkeit, mit der Informationen verteilt, übertragen oder veröffentlicht werden, hat in den letzen Jahren rasant zugenommen. Dadurch wurde das Wachstum eines Marktes ermöglicht, der die Bedeutung und den Marktwert von persönlichen Daten fokussiert (Bohl, Manouchehri et al. 2007: 27ff.). Für die Betreiber von Web 2.0-Publikumsdiensten sind diese Nutzerdaten Basis ihres Geschäftsmodells. Eine Plattform hat umso mehr Erfolgspotenzial, je größer ihr Nutzerkreis ist und je mehr Daten auf der Plattform zu finden sind. Kommerzialisierung und Datenmissbrauch liegen hier eng beieinander, denn schnell lassen sich mit Hilfe gesammelter Informationen persönliche Profile von Nutzern erstellen. Die auf Flickr.com verfügbaren persönlichen Bilder von Urlaubsreisen oder besuchten Events erlauben beispielsweise eine zeitliche Einordnung und illustrieren so die Entwicklung einer Person. Private Weblogs,

StudiVZ.net oder MySpace.com können über die politische Einstellung und die individuellen Interessen der Nutzer Aufschluss geben. Plattformen wie Del.icio.us präsentieren Bookmarks und Amazon.de veröffentlicht die „Wunschzettel" der Nutzer. Diese Daten stehen öffentlich zur Verfügung und können (kommerziell) verwertet werden. Durch die fortschreitende Oligopolisierung auf Anbieterseite erlangen international operierende Kommunikationskonzerne außerdem durch Kombinationen von Daten unterschiedlicher Plattformen komplexe Nutzerprofile. Die Entwicklung des Web 2.0 bringt also fast zwangsläufig eine Welle von Datenmissbrauchsgefahren mit sich. Dadurch, dass den Betreibern der Dienste persönliche Daten preisgegeben wurden, haben diese die Möglichkeit, die Daten zu ihrem ökonomischen Vorteil zu verwenden.

2. Web 2.0 und Social Software

Nachdem im Jahr 2001 der Zusammenbruch der New Economy den Blütenträumen der Branche ein jähes Ende gesetzt hatte, kehrten Optimismus und Aufschwung in den letzten Jahren in den Internet-Sektor zurück (NZZ-Online 2006). Heutzutage wird Startups wieder Risikokapital zur Verfügung gestellt, um auf der Welle des „Buzzword" Web 2.0 mit zu reiten (Hippner 2006: 5). Unter diesem Begriff entwickelte sich in den letzen Jahren ein Boom, der auf grundlegenden Veränderungen hinsichtlich der Wahrnehmung des World Wide Web basiert. Die heute weit verbreitete Bezeichnung der zweiten Generation des Internet-Geschäfts ist auf ein Brainstorming von Tim O'Reilly und Dale Dougherty, Mitbegründer von „O'Reilly Media" und Herausgeber des MAKE Magazins, sowie Graing Cline von „Media-Live" zurückzuführen. Der Verleger Tim O'Reilly veranstaltete im Jahr 2004 eine Konferenz, auf der

Prinzipien von Webdiensten analysiert und identifiziert wurden, die den Crash der New Economy überlebt hatten und nun erneut erfolgreich im Geschäft waren (O'Reilly 2005). Allerdings hatte Tim O'Reilly es zunächst versäumt, eine konkrete Definition dieses Begriffs zu veröffentlichen. Abbildung 1 zeigt einige Facetten des Begriffs und verdeutlicht dessen Unschärfe.

Abbildung 1: Web 2.0 – Tag-Cloud (Angermeier 2005).

Demzufolge ist sowohl das Verständnis als auch die Interpretation des Begriffs „Web 2.0" letztlich jedem Nutzer, Betreiber und Experten selbst überlassen. In den letzten Jahren haben sich allerdings unter zahlreichen Definitionen und Kommentaren einige herauskristallisiert, die wichtige Inhalte aufgreifen und zusammenfassen. Tim O'Reilly veröffentlichte Ende 2005 selbst eine eigene Definition:

Definition	„Web 2.0 is the network as platform, spanning all connected devices; Web 2.0 applications are those that make the most of the intrinsic advantages of that platform: delivering software as a continually-updated service that gets better the more people use it, consuming and remixing data from multiple sources, including individual users, while providing their own data and services in a form that allows remixing by others, creating network effects through an "architecture of participation," and going beyond the page metaphor of Web 1.0 to deliver rich user experiences."(O´Reilly 2005)

Kommentare	„Web 2.0 is any web page that can be spammed." (Wall 2006) „… a piece of jargon, nobody even knows what it means." (Berners-Lee 2006) "…ist der Versuch, neue Strömungen im Netz zusammen zu fassen und ihnen einen Begriff zu geben." (Kaul 2005)

Das Resultat dieses „neuen" Webs ist das Erlangen einer gemeinsamen und geteilten Intelligenz – hervorgerufen durch die Vernetzung, die Interaktivität und die Offenheit für die Nutzer. Eine Redaktion, die Texte verfasst, wird durch den Nutzer ersetzt, da jeder die Möglichkeit hat, in die Rolle des Redakteurs zu schlüpfen. Das Web 2.0 wird geprägt durch den User-generated Content. Diese Inhalte sind für Unternehmen von großem Wert, denn sie helfen, zielgruppenorientierte Informationen dynamisch zu beschaffen, um eine bessere Marktstellung zu erlangen (Baur & Mandl 2007: 88).

Deswegen erfolgt die dynamische Entwicklung der Web 2.0-Dienste zielgruppenspezifisch. Damit eng verbunden ist auch die Tatsache, dass viele Anwendungen im Beta-Status (perpetual beta) verweilen. Dies ist sowohl auf die stete Änderung und Ausweitung der Zielgruppen in diesem Sektor als auch auf die neuen geforderten Ansprüche der Nutzer und die kontinuierliche Weiterentwicklung von Anwendungen zurückzuführen. Die offenen Schnittstellen einzelner Anwendungen gestatten die Integration verschiedener Dienste/Mash-Ups: So ist es beispielsweise Bloggern möglich, eine Google-Map direkt im Weblog darzustellen. Zuletzt ist die Verlagerung von Desktop- zu Web-Anwendungen zu nennen: So enthalten viele Web-Anwendungen vergleichbare Funktionen wie fest installierte Desktop-Programme.

Es ist allerdings ein Irrtum, zu glauben, dass der Anhang „2.0“ für eine technische Weiterentwicklung des bestehenden Produkts steht, wie dies sonst in der Softwarebezeichnung üblich ist. Es sind zwar einige technische Neuheiten entwickelt worden, jedoch verbirgt sich hinter der Bezeichnung „Web 2.0“ im Wesentlichen eine inhaltliche Veränderung. Deutlich ist zu erkennen, dass die Transformation von Web 1.0 zu Web 2.0 in erster Linie auf den Entwicklungen innovativer Anwendungen basiert, was eine Ablösung älterer Dienste zur Folge hat. In diesem Zusammenhang wird sowohl dem Menschen als Nutzer als auch seinem sozialen Beziehungsnetz eine bedeutende Rolle zugewiesen. Die Nutzer befinden sich nun im Zentrum des Entstehungsprozesses und können sich aktiv an ihm beteiligen. Sie werden zu Co-Entwicklern und können an der Umgebung partizipieren.

Social Software wird meist mit dem Begriff „Web 2.0“ in Zusammenhang gebracht oder gar gleichgesetzt. Eine Zuordnung als Teilmenge des Web 2.0 scheint allerdings am geeignetsten zu sein. Auch hier lässt sich, ähnlich wie

beim Begriff „Web 2.0“, keine eindeutige Definition finden. Allerdings gibt das Wort „Social“ Hinweise auf den Fokus und die Zielgruppe. In dieser Arbeit soll folgende Definition von Hippner übernommen werden (Hippner 2006: 7): „Social Software umfasst webbasierte Anwendungen, die für Menschen den Informationsaustausch, den Beziehungsaufbau und die Kommunikation in einem sozialen Kontext unterstützen und sich an spezifischen Prinzipien orientieren.“

Die in der Definition zuvor genannten spezifischen Prinzipien stellen ein „Bündel“ dar und charakterisieren nach Hippner den „Geist“ der Social Software:

- Im Mittelpunkt der Social Software steht das Individuum/die Gruppe.
- Social Software unterliegt der Grundidee der Selbstorganisation.
- Es wird eine soziale Rückkopplung (Social Feedback) in Form von Social Ratings (Zahl der Querverweise, Kommentare etc.) unterstützt.
- Der Fokus liegt weniger auf der einzelnen Information, sondern vielmehr auf der Struktur, die sich aus der Verknüpfung der Informationen ergibt.
- Das Individuum integriert sich in die Gruppe, d.h. eine reine „One-to-One“-Kommunikation ist nicht erwünscht.
- Personen, Beziehungen, Inhalte und Bewertungen sollen sichtbar gemacht werden.

Eine Einordnung einiger Social Software-Anwendungen ist Abbildung 2 zu entnehmen. Die Zuordnung der einzelnen Anwendungen zu einem der drei Schwerpunkte erfolgt nicht zwangsläufig und ist auch nicht eindeutig. Sie sind

je nach Begriffsinterpretation durchaus im Zieldreieck verschiebbar und unterliegen einer gewissen Flexibilität (Hippner 2006: 8).

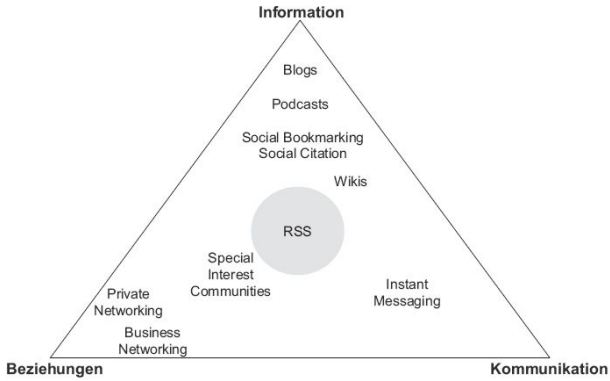

Abbildung 2: Klassifikationsschema von Social Software (in Anlehnung an Hippner 2006: 9).

2.1 Anwendungsschwerpunkt „Information“

Um Nutzern Informationen zur Verfügung zu stellen, wird im Web 2.0 häufig auf Weblog-Methoden zurückgegriffen. Hierbei werden sowohl in geregelten Abständen als auch sporadisch neue Artikel oder Einträge veröffentlicht. Die intuitive Bedienbarkeit steht im Vordergrund, so dass dem Nutzer via Themenklassifikation oder Veröffentlichungsdatum ein leichter Zugang zu den Artikeln oder Einträgen gewährleistet wird. Inhaltlich charakteristisch für Weblogs ist häufig ein hoher Grad an Subjektivität und Individualität, insbesondere dann, wenn sie von Privatpersonen betrieben werden. So können Weblogs Tagebücher oder Diskussionsbeiträge zu fachspezifischen Themen beinhalten. Auch Weblogs von Unternehmen dienen als Informationsquellen und werden mehr und mehr eingesetzt. Die starke Vernetzung und Kommentierung einzelner Weblogs steht im Vordergrund, wodurch die Interaktion

zwischen den Nutzern ermöglicht wird. Ähnlich zu Weblogs können Podcasts dem Anwendungsschwerpunkt Information zugeordnet werden. Podcasts stellen Information nicht schriftlich, sondern als gesprochenes Wort in Form einer (meist) MP3-Datei zur Verfügung. Bislang steht auch hier im Regelfall bei den Produzenten eine nicht kommerzielle Motivation im Vordergrund. Diese Art der Informationsverbreitung weist ein hohes Marktpotenzial auf, so dass mehr und mehr Unternehmen darauf zurückgreifen, um so ihrer Zielgruppe Neuigkeiten anzubieten (Hippner 2006: 10ff.).

2.2 Anwendungsschwerpunkt „Beziehung“

In diesem Anwendungsfeld ist zwischen privaten und geschäftlichen Netzwerken zu unterscheiden. Gemein ist beiden, dass ihre Themenschwerpunkte bei den Social Network Services liegen, die als Verbund einer Online Community agieren: Hier wird den Nutzern die Möglichkeit gegeben, sich auf einer einheitlichen Plattform auszutauschen. Die Basiskonzepte sind bei den entsprechenden Diensten ähnlich. So erstellt der Nutzer nach bzw. bei der Registrierung ein Profil seiner Person. Je nach Dienst und Zielgruppe enthält das erfragte Profil unterschiedlich umfangreiche soziodemografische Daten respektive Informationen zu Interessen oder Fähigkeiten der jeweiligen Person. Welche Daten für die Profilerstellung abgefragt werden, richtet sich danach, ob in der Community der Networking-Charakter im Vordergrund steht und der Fokus auf der Erweiterung privater bzw. geschäftlicher Kontakte liegt (Hippner 2006: 13ff.).

2.3 Anwendungsschwerpunkt „Kommunikation“

Bei den zuvor genannten Anwendungen geht es um den kommunikativen Austausch. Bei den Diensten, die diesem Pol zugeordnet werden sollen, steht jedoch die Kommunikation im Sinne der Echtzeitkommunikation im Vordergrund. Sogenannte Instant Messaging Dienste, wie zum Beispiel twitter.com, ermöglichen dabei in der Regel textuelle Kommunikation (Hippner 2006: 14ff.).

Festzuhalten ist, dass Social Software offenbar nicht nur einen kurzfristigen Trend, sondern vielmehr einen langfristigen Wandel im Zeitalter der Kommunikation eingeleitet hat. Das Web 2.0 hat neben Social Software zahlreiche weitere Angebote der interaktiven Mitgestaltung zu bieten, insbesondere die bereits zuvor erwähnte Auslagerung von bisher desktop-orientierten Diensten zu webbasierten Anwendungen.

3. Gefahr des Datenmissbrauchs

Die möglichen Gefahren, die mit dem Sektor Web 2.0 und Social Software verbunden sind, lassen sich zwar teilweise erahnen, doch inwieweit aus den veröffentlichten personenbezogenen Daten Gefahren des Datenmissbrauchs resultieren, ist meist nicht direkt ersichtlich. Eine Aufstellung relevanter personenbezogener Daten findet sich in der nachfolgenden Tabelle:

Name	Geburtstag	Land
Sprache	Telefonnummer	E-Mail
Universität	Anschrift	Qualifikation
Bildung	Fotos	Kontakte
Interessen	Politische Einstellung	Webseite
Arbeitgeber	Beruf	...

Tabelle 1: Auswahl personenbezogener Merkmale.

Daten können über zwei unterschiedliche Aktivitäten ins Netz gelangen: Zum einen kann der Nutzer explizit Daten veröffentlichen. Dies erfolgt über die Registrierung bei einem Dienst. Hier werden die vom Nutzer bewusst veröffentlichten Daten personenbezogen in seinem Profil gespeichert. Inwieweit diese Daten nun für andere Nutzer sichtbar sind, ist abhängig vom jeweiligen Dienst und dessen Offenlegungspolitik. Die andere Möglichkeit ist jene dem Nutzer unbewusste Variante, bei der Daten durch das automatisierte, im Hintergrund ablaufende Beobachten des Nutzerverhaltens (Tracking) ermittelt und – zumindest beim Dienstbetreiber – gespeichert werden, um daraus später Rückschlüsse zu ziehen.

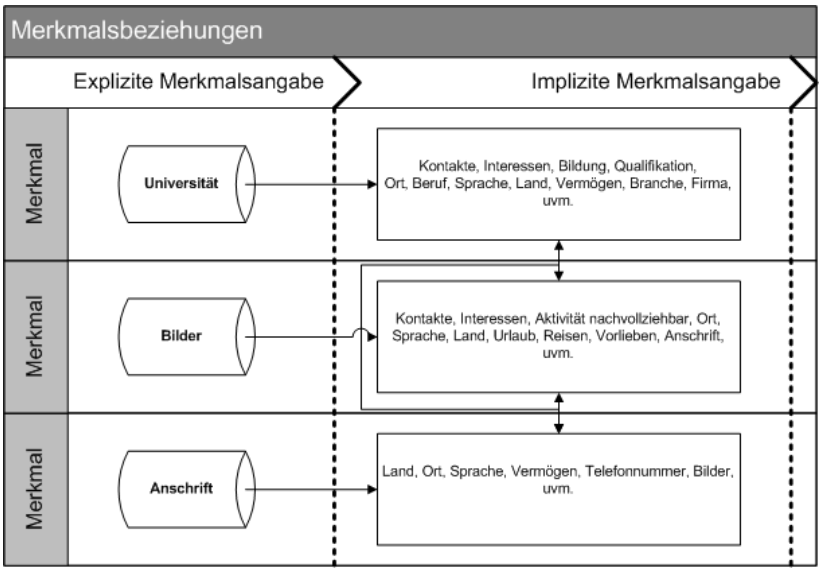

Abbildung 3: Explizite und implizite Merkmalsbeziehungen.

In Abbildung 3 werden exemplarisch drei explizite Merkmalsangaben und damit verbundene, implizite Merkmalsbeziehungen dargestellt. Bei Angabe der Universität, die ein Nutzer besucht, sind beispielsweise der Ort, die Region und das Land, in der sich der Nutzer aufhält, ermittelbar, auch wenn er diese Angaben nicht explizit tätigt. Ferner sind Rückschlüsse auf Qualifikationen, Bildung und Interessen denkbar.

4. Gefahren bei gleichzeitiger Nutzung verschiedener Dienste

Bisher gewährleisteten Dienste ihren Nutzern zumindest ein gewisses Maß an Datenschutz, da die Daten meist nur für angemeldete Nutzer eben dieses einen Dienstes sichtbar waren. Die jedoch im August 2007 online gestellte Suchmaschine Spock.com setzt gerade diesen Schutz außer Kraft (Golem 2007). Das Start-up-Unternehmen aus den USA entwickelte eine Suchmaschine, die Informationen zu Personen findet. Das zugrunde liegende Konzept fußt auf einer Kombination von Web 2.0-Elementen und Google. Die Absichten von Spock.com sind laut Aussage des Mitbegründers Jay Bhatti, „Ergebnisse rund um den Menschen präsentieren zu wollen und sich auf diese Weise von anderen Suchmaschinen zu unterscheiden, da die Ausrichtung nur auf Menschen basiert“ (Golem 2007). Spock.com durchforstet Suchmaschinen und Social Software Dienste, um an die Daten der Nutzer zu kommen und diese Informationen der Öffentlichkeit zugänglich zu machen. Die Vielzahl an Suchfunktionen erlaubt es, nach Namen (auch bei nicht exakter Angabe), E-Mail-Adresse, Geschlecht, Alter, Ort oder anderen Schlagwörtern zu suchen. Welche Gefahren die Kombination von Diensten bergen kann, verdeutlichen die nachfolgenden zwei fiktiven Szenarien:

Szenario 1 bildet die Situation ab, dass ein Nutzer sowohl den Bilderdienst Flickr.com als auch das Kommunikationsportal ICQ nutzt. Die verschiedenen Merkmalsanzeigen der in diesem Szenario verglichenen Dienste fallen unterschiedlich aus: So besteht bei Flickr.com nicht die Möglichkeit, den Geburtstag, die Telefonnummer, den Bildungsgrad und die Firma eines Nutzers abzufragen. Ist jedoch dieser Nutzer bei ICQ administriert, so würde spock.com durch das Matching der Daten gerade diese Datenlücken füllen können. Diese zusätzliche Informationsgewinnung ist als eine Form des Datenmissbrauchs anzusehen, da die Daten des jeweiligen Nutzers von einem Dritten, in diesem Fall einer Suchmaschine, zweckentfremdet und weiterverarbeitet werden.

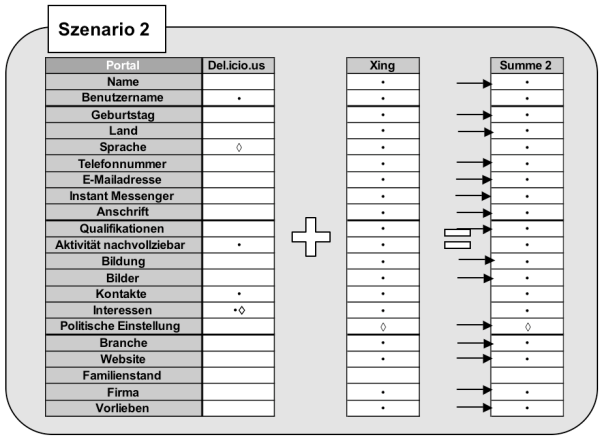

Abbildung 4: Veränderung der Informationsdichte bei Kombination mehrerer Web 2.0-Dienste.

Szenario 2 illustriert die Situation, in der ein Nutzer ursprünglich den Social Bookmark-Dienst Del.icio.us nutzt und dessen dort abrufbare Daten um Informationen zum gleichen Nutzer aus dem Business-Netzwerk xing.com ergänzt werden. Der durch diese Kombination erlangte zusätzliche

Informationsgewinn fällt deutlich höher aus und wird beispielhaft in Abbildung 4 dargestellt.

Die Nutzung eines Dienstes führt demzufolge nicht zwangsläufig zu einer hohen Informationspreisgabe. Bei kombinierter Nutzung verschiedener Dienste steigt diese Gefahr jedoch erheblich. Die Gefahren des Datenmissbrauchs sind also im Fall der Nutzung mehrerer Dienste deutlich größer. Nutzer verschiedener Dienste laufen Gefahr, die Menge, das Ausmaß und die Folgen ihrer Merkmalsanzeigen nicht mehr abschätzen zu können. Das resultierende Risiko des Datenmissbrauchs steigt beträchtlich an, da mittels neuer Suchdienste eine solche zweckentfremdete Merkmalsanzeige durch Dritte abfragbar ist.

5. Konzepte und Strategien zur Vorbeugung von Datenmissbrauch

Die zuvor aufgeführten Gefahren verdeutlichen einmal mehr, dass der Datenschutz zu einem zentralen Thema geworden ist und zudem weiter ausgebaut werden sollte. Es ist den wenigsten Nutzern bewusst, wo sie bei der Nutzung globaler Dienste und Plattformen Datenspuren hinterlassen und wie diese ausgewertet werden. Die daraus resultierende Verunsicherung der Nutzer und deren Bedenken bezüglich des Datenschutzes gehören auch weiterhin zu den größten Hemmnissen des E-Commerce (Köhntopp & Pfitzmann 2001: 2). Hier sollen drei Konzepte und Strategien (Krasemann 2006: 211) zur Vorbeugung von Datenmissbrauch kurz vorgestellt und diskutiert werden:

Die erste Form ist das Accounting. Sie ermöglicht Unternehmen und Organisationen, Kunden- und Mitarbeiterdaten zu verwalten. Dabei werden extern

bzw. passiv Daten verwaltet, ohne dass der jeweils verwaltete Nutzer Einfluss darauf nehmen kann.

Die zweite Form wird durch das sogenannte Profiling beschrieben. Auch hier erfolgt eine externe Verwaltung der Nutzerdaten. Sie dient dem Tracking des Nutzerverhaltens, um Kunden besser erfassen und gezielter ansprechen zu können. Auch diese Form wird von Unternehmen gewählt und bietet dem Nutzer keine Einflussmöglichkeit.

Ein sehr umfassender Ansatz für ein Datenschutzkonzept ist das Identitätsmanagement (Koch & Möslein 2005: 12), das insbesondere von Datenschützern propagiert wird. Es handelt sich dabei um ein selbstgesteuertes und somit internes Identitätsmanagement. Der einzelne Nutzer verwaltet sein Auftreten in unterschiedlichen Rollen gegenüber Kommunikationspartnern selbst. Dabei kann er durch eine Verwaltungssoftware unterstützt werden; eine weitere einfache Option ist die Verwendung von Pseudonymen.

In diesem Beitrag bezeichnet das Identitätsmanagement einen zielgerichteten und bewussten Umgang mit Identitäten, Anonymitäten und Pseudonymitäten, der intern und aktiv durch den Nutzer selbst realisiert wird (Kuhlenkamp & Manouchehri et al. 2006: 31). Die Strategie des Identitätsmanagements basiert auf der Verwaltung von Teilidentitäten sowie implizit ins Netz gelangten Daten. Teilidentitäten verstehen sich dabei als Untermengen der Identitätsinformation. Sie repräsentieren die Person bzw. den Nutzer im jeweils zugehörigen Kontext (Köhntopp & Pfitzmann 2001: 3), was in nachfolgender Abbildung 5 dargestellt ist:

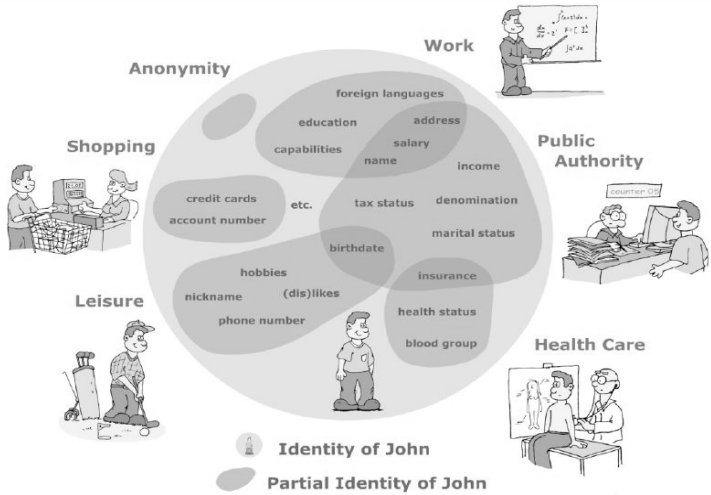

Abbildung 5: Teilidentitäten – verdeutlicht am Beispiel einer fiktiven Person (Pfitzmann & Borcea-Pfitzmann 2005: 2).

Die Verwaltung dieser Teilidentitäten beinhaltet sowohl die eigentlichen personenbezogenen Daten als auch den Teil der Information, die den Bezug oder Verweis zur jeweiligen Person herstellen (Köhntopp 2000: 8). Es ist allerdings zu erwähnen, dass ein Identitätsmanagementsystem in der Obhut des jeweiligen Nutzers liegt, also nicht in der Kontrolle des Dienstleistungsanbieters stehen sollte.

Ein umfassendes Identitätsmanagementsystem regelt die Verwendung personenbezogener Daten (Hansen, Krasemann et al. 2003: 551). Im deutschen Recht bezeichnet die informationelle Selbstbestimmung das Recht des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner personenbezogenen Daten zu bestimmen (Tinnefeld, Ehmann et al. 1998: 3).

Es handelt sich dabei nach der Rechtsprechung des Bundesverfassungsgerichts um ein Grundrecht.

Mechanismen zur erfolgreichen Umsetzung eines Identitätsmanagements basieren auf den Datenschutzgrundsätzen der Datensparsamkeit und der Transparenz. Kernelemente sind in diesem Zusammenhang Verfahren zur Gewährleistung von Anonymität und Pseudonymität. Weitere spezielle Aufgaben können dabei von dritten Parteien übernommen werden, wobei die Aktivität vom Nutzer selbst ausgeht (Köhntopp & Pfitzmann 2001: 3).

Anonymität kann als Zustand definiert werden, in dem eine Person innerhalb einer Menge von Personen – der Anonymitätsmenge – nicht zu identifizieren ist (Pfitzmann & Köhntopp 2001: 1). Eine ausreichend große Anonymitätsmenge sollte die Basis des Identitätsmanagements sein. Dadurch wird gewährleistet, dass kein personenbezogener Datenfluss außerhalb des Identitätsmanagementsystems den Datenschutz gefährdet (Köhntopp & Pfitzmann 2001: 3). Ein weiterer Vorteil ergibt sich, wenn diese Anonymität von einem allgemeinen Systemdatenschutz garantiert wird (Berthold, Federrath et al. 2001: 117).

An dieser Stelle sei angemerkt, dass die Nutzung von Komponenten aus dem Anwendungsschwerpunkt „Beziehung“, z.B. in Form von privaten und geschäftlichen Netzwerken, der Anonymität entgegensteht. Social Networks benötigen die Preisgabe persönlicher Informationen, da ohne diese kein Netzwerkaufbau erfolgen kann. Die nutzerzentrierte Ausrichtung aktueller Social Networks verhindert also den Einsatz des Konzepts der Anonymität zur Vorbeugung von Datenmissbrauch. Würde der Aufbau hingegen inhaltszentriert erfolgen, wäre Anonymität theoretisch realisierbar. Aktuelle Forschungen zur

Superdistribution zeigen hier erste Möglichkeiten auf (Streng, Ahrens et al. 2008: 69ff.).

Das Spektrum zwischen Anonymität und eindeutiger Identifizierbarkeit kann als Pseudonymität definiert werden (Köhntopp & Pfitzmann 2001: 4). Dabei versteht man unter einem Pseudonym im weiteren Sinne einen Schlüssel, der den Pseudonyminhaber mit seinen Daten in Verbindung bringt.

Die Anonymität eines Pseudonyminhabers ist dabei von der Anzahl der direkten Zuordnungen des Pseudonyms zur realen Person abhängig. Ferner ist für eine Zuordnung die Pseudonymverwendung ausschlaggebend. Diese Zuordnung kann etwa durch einen Personenbezug mit Hilfe der Beobachtung einer Verkettung einzelner Aktionen hergestellt werden (Köhntopp & Pfitzmann 2001: 4).

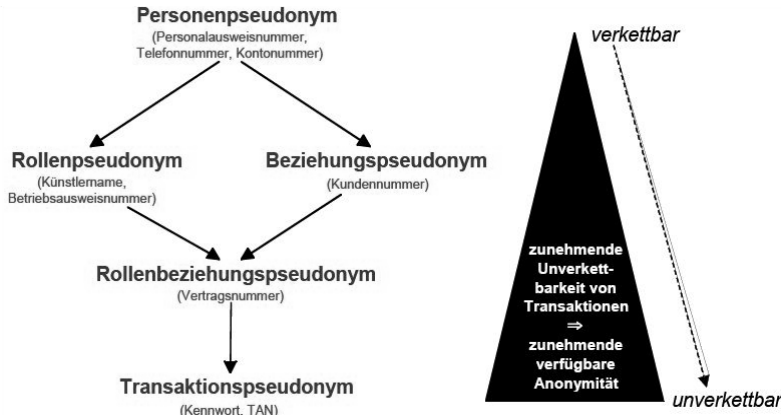

Abbildung 6: Pseudonymarten und ihr Verwendungszusammenhang (Pfitzmann & Borcea-Pitzmann 2005: S. 7).

Der Grad der Anonymität ist generell abhängig von der Pseudonymklasse. So gestatten Rollen- und Beziehungspseudonyme gegenüber Personenpseudonymen mehr Anonymität. Der jeweilige Grad an Anonymität steigt bei der Verwendung von Rollenbeziehungspseudonymen. Transaktionspseudonyme ermöglichen ihren Nutzern den höchsten Grad an Anonymität (Pfitzmann & Borcea-Pitzmann 2005: 7).

Ein weiteres Konzept stellt das Personal Information Management dar, welches die Verwaltung persönlicher Daten unterstützt (Hansen & Neumann 2002: 45). Die hierfür notwendige Software kann sowohl bei Einzelpersonen als auch in Netzwerken Anwendung finden und sorgt dafür, dass der einzelne Nutzer eigene Daten verwalten kann, aber gleichzeitig nicht alle Benutzer diese Daten vollständig einsehen oder bearbeiten können (Kuhlenkamp, Manouchehri et al 2006: 31ff.).

Auch das Personal Information Management-Konzept bietet keine vollständige Sicherheit, da das Anwendungsgebiet nicht mit allen Web 2.0-Publikumsdiensten und Social Software übereinstimmt. Es dient eher der Verwaltung und Organisation personenbezogener Daten in E-Mail-, Kalender- und Notizapplikationen (Kuhlenkamp, Manouchehri et al. 2006: 31).

Ein neuer Ansatz könnte das Speichern von Daten unter Berücksichtigung eines Verfallsdatums sein. Entsprechende Vorschläge sehen vor, dass jegliche persönlichen Daten, die im Internet verwendet werden, von Gesetzes wegen mit einer zeitlichen Befristung versehen werden. Nach Ablauf der Frist sind die Daten durch den Betreiber automatisiert zu löschen, sofern durch den Nutzer nicht eine erneute Freigabe erfolgt. Hier ist von technischer Seite „lediglich“ das Datenmodell der Web 2.0-Dienste anzupassen. Die rechtliche Durchsetzung solcher Bestimmungen erscheint jedoch schwierig.

Um einen hohen Schutz der eigenen Daten in Anwendungen der Web 2.0-Publikumsdienste und Social Software sicherzustellen, ist den Nutzern – neben den zuvor vorgestellten Konzepten – der sorgfältige und sparsame Umgang mit ihren persönlichen Daten zu raten. Je weniger sie von sich preisgegeben, desto geringer ist die Gefahr von Datenmissbrauch (Wege 2002: 79). Es liegt vor allem in der Hand der Nutzer, welchen Sicherheitsstandard sie für ihre persönlichen Daten erreichen. Zudem ist ein Blick in die AGB der Anbieter zu empfehlen. Ein umfassender und vollständiger Schutz kann aber trotz allem nie garantiert werden. Verbleibende Restrisiken werden bei Nutzung der Dienste und Portale immer bestehen. Die Nutzer über diese Risiken ausreichend zu informieren, obliegt in Zeiten der modernen Mediennutzung auch den Medien selbst.

Literaturverzeichnis

Alby, T. (2007): Web 2.0 – Konzepte, Anwendungen, Technologien. Hanser, München.

Angermeier, M. (2005): Netz 2.0. Online im Internet: http://blog.aperto.de/2005/11/24/netzwelt-web-20/netz20-das-web20-auf-gut-deutsch-22/ [Abrufdatum 10.12.2007].

Bauer, N.; Mandl, P. (2007): Agiles Informationsmanagement. In: HMD – Praxis der Wirtschaftsinformatik (Heft 255): 88-96.

Berners-Lee, T. (2006): developerWorks Interviews: Tim Berners-Lee. Online im Internet: http://www-128.ibm.com/developerworks/podcast/dwi/cm-int082206.txt [Abrufdatum 03.12.2007].

Berthold, O.; Federrath, H.; Köpsell, S. (2001): Web MIXes: A system for anonymous and unobservable Internet access. In: Lecture Notes in Computer Science – Designing Privacy Enhancing Technologies: 115-129.

Bohl, O.; Manouchehri, S., Winand, U. (2007): Unternehmerische Wertschöpfung im Web 2.0. In: HMD – Praxis der Wirtschaftsinformatik (Heft 255): 27-36.

Golem (2007): Spock.com: Suchmaschine findet Personen. Indexierung von Milliarden Menschen geplant. Online im Internet: http://www.golem.de/0708/53993.html. [Abrufdatum 04.01.2008].

Hansen, H.; Neumann, G. (2002). Arbeitsbuch Wirtschaftsinformatik. UTB, Stuttgart.

Hansen, M.; Krasemann, H.; Rost, M.; Genghini, R. (2003): Datenschutzaspekte von Identitätsmanagementsystemen. In: Datenschutz und Datensicherheit (Heft 27): 551-555.

Hippner, H. (2006): Bedeutung, Anwendungen und Einsatzpotenziale von Social Software. In: HMD – Praxis der Wirtschaftsinformatik (Heft 252): 6-16.

Kaul, K. (2005): Web 2.0 – Phantom oder Phänomen? Online im Internet: http://www.dw-world.de/dw/article/0,2144,1790308,00.html [Abruf-datum 07.12.2007].

Koch, M.; Möslein, K. (2005): Identities Management for E-Commerce and Collaboration Applications. In: International Journal of Electronic Commerce (Heft 9): 11-29.

Köhntopp, M. (2000): Identitätsmanagement - ein neues, altes Konzept. In: Datenschutz-Nachrichten (Heft 3): 7-12.

Köhntopp, M.; Pfitzmann, A. (2001): Informational Self-Determination by Identity Management. In: it – Information Technology (Heft 5): 227-235.

Krasemann, H. (2006): Selbstgesteuertes Identitätsmanagement – Rechtliche Möglichkeiten der Nutzung verschiedener Identitäten. In: Datenschutz und Datensicherheit 30 (Heft 4): 211-214.

Kuhlenkamp, A.; Manouchehri, S.; Mergel, I.; Winand, U. (2006): Privatsphäre versus Erreichbarkeit bei der Nutzung von Social Software. In: HMD – Praxis der Wirtschaftsinformatik (Heft 252): 27-35.

NZZ-Online (2006): Zukunft 2.0. Online im Internet: www.nzz.ch/2006/01/13/em/articleDHFG7.print.html. [Abrufdatum 10.12.2007].

O'Reilly, T. (2005): What is Web 2.0? Online im Internet: www.oreillynet.com/pub/a/oreilly/tim/news/2005/09/30/what-is-web-20.html. [Abrufdatum 10.12.2007].

Pfitzmann, A.; Borcea-Pfitzmann, K. (2005): Identitätsmanagement und informationelle Selbstbestimmung. In: Roßnagel, A. (Hrsg.): Allgegenwärtige Identifizierung? Neue Identitätsinfrastrukturen und ihre rechtliche Gestaltung. Nomos, Baden-Baden: 83-91.

Streng, S.; Ahrens, S.; Anton, K.; Küpper, A. (2008): Inhaltszentrierte Virtuelle Gemeinschaften. In: Meißner, K.; Engelien, M. (Hrsg.): Virtuelle Organisation und Neue Medien 2008. TUDpress, Dresden, 2008: 69-78.

Tinnefeld, M.-T.; Ehmann, E. et al. (1998): Einführung in das Datenschutzrecht. Oldenbourg, München.

Wall. (2006): Web 2.0 – A Definition. Online im Internet: http://stigmergicweb.org/2006/11/29/web-20-a-definition/ [Abrufdatum 01.12.2007].

Wege, J. (2002): Datenmissbrauch: Haftung und Schutz – Datensicherheit ist auch eine verfassungsrechtliche Aufgabe. In: Versicherungsbetriebe (Heft 5): 79.